

EC-Council

Exam Questions 212-89

EC Council Certified Incident Handler (ECIH v2)



NEW QUESTION 1

Which of the following terms may be defined as “a measure of possible inability to achieve a goal, objective, or target within a defined security, cost plan and technical limitations that adversely affects the organization’s operation and revenues?”

- A. Risk
- B. Vulnerability
- C. Threat
- D. Incident Response

Answer: A

NEW QUESTION 2

A distributed Denial of Service (DDoS) attack is a more common type of DoS Attack, where a single system is targeted by a large number of infected machines over the Internet. In a DDoS attack, attackers first infect multiple systems which are known as:

- A. Trojans
- B. Zombies
- C. Spyware
- D. Worms

Answer: B

NEW QUESTION 3

An organization faced an information security incident where a disgruntled employee passed sensitive access control information to a competitor. The organization’s incident response manager, upon investigation, found that the incident must be handled within a few hours on the same day to maintain business continuity and market competitiveness. How would you categorize such information security incident?

- A. High level incident
- B. Middle level incident
- C. Ultra-High level incident
- D. Low level incident

Answer: A

NEW QUESTION 4

Identify the malicious program that is masked as a genuine harmless program and gives the attacker unrestricted access to the user’s information and system. These programs may unleash dangerous programs that may erase the unsuspecting user’s disk and send the victim’s credit card numbers and passwords to a stranger.

- A. Cookie tracker
- B. Worm
- C. Trojan
- D. Virus

Answer: C

NEW QUESTION 5

An incident recovery plan is a statement of actions that should be taken before, during or after an incident. Identify which of the following is NOT an objective of the incident recovery plan?

- A. Creating new business processes to maintain profitability after incident
- B. Providing a standard for testing the recovery plan
- C. Avoiding the legal liabilities arising due to incident
- D. Providing assurance that systems are reliable

Answer: A

NEW QUESTION 6

Risk is defined as the probability of the occurrence of an incident. Risk formulation generally begins with the likeliness of an event’s occurrence, the harm it may cause and is usually denoted as Risk = ?(events)X (Probability of occurrence)X?

- A. Magnitude
- B. Probability
- C. Consequences
- D. Significance

Answer: A

NEW QUESTION 7

Computer forensics is methodical series of techniques and procedures for gathering evidence from computing equipment, various storage devices and or digital media that can be presented in a course of law in a coherent and meaningful format. Which one of the following is an appropriate flow of steps in the computer forensics process:

- A. Examination > Analysis > Preparation > Collection > Reporting
- B. Preparation > Analysis > Collection > Examination > Reporting

- C. Analysis > Preparation > Collection > Reporting > Examination
- D. Preparation > Collection > Examination > Analysis > Reporting

Answer: D

NEW QUESTION 8

Multiple component incidents consist of a combination of two or more attacks in a system. Which of the following is not a multiple component incident?

- A. An insider intentionally deleting files from a workstation
- B. An attacker redirecting user to a malicious website and infects his system with Trojan
- C. An attacker infecting a machine to launch a DDoS attack
- D. An attacker using email with malicious code to infect internal workstation

Answer: A

NEW QUESTION 9

Computer Forensics is the branch of forensic science in which legal evidence is found in any computer or any digital media device. Of the following, who is responsible for examining the evidence acquired and separating the useful evidence?

- A. Evidence Supervisor
- B. Evidence Documenter
- C. Evidence Manager
- D. Evidence Examiner/ Investigator

Answer: D

NEW QUESTION 10

Identify a standard national process which establishes a set of activities, general tasks and a management structure to certify and accredit systems that will maintain the information assurance (IA) and security posture of a system or site.

- A. NIASAP
- B. NIAAAP
- C. NIPACP
- D. NIACAP

Answer: D

NEW QUESTION 10

One of the main objectives of incident management is to prevent incidents and attacks by tightening the physical security of the system or infrastructure. According to CERT's incident management process, which stage focuses on implementing infrastructure improvements resulting from postmortem reviews or other process improvement mechanisms?

- A. Protection
- B. Preparation
- C. Detection
- D. Triage

Answer: A

NEW QUESTION 15

Organizations or incident response teams need to protect the evidence for any future legal actions that may be taken against perpetrators that intentionally attacked the computer system. EVIDENCE PROTECTION is also required to meet legal compliance issues. Which of the following documents helps in protecting evidence from physical or logical damage:

- A. Network and host log records
- B. Chain-of-Custody
- C. Forensic analysis report
- D. Chain-of-Precedence

Answer: B

NEW QUESTION 17

A security policy will take the form of a document or a collection of documents, depending on the situation or usage. It can become a point of reference in case a violation occurs that results in dismissal or other penalty. Which of the following is NOT true for a good security policy?

- A. It must be enforceable with security tools where appropriate and with sanctions where actual prevention is not technically feasible
- B. It must be approved by court of law after verifications of the stated terms and facts
- C. It must be implemented through system administration procedures, publishing of acceptable use guide lines or other appropriate methods
- D. It must clearly define the areas of responsibilities of the users, administrators and management

Answer: B

NEW QUESTION 22

Incident handling and response steps help you to detect, identify, respond and manage an incident. Which of the following helps in recognizing and separating the infected hosts from the information system?

- A. Configuring firewall to default settings
- B. Inspecting the process running on the system
- C. Browsing particular government websites
- D. Sending mails to only group of friends

Answer: B

NEW QUESTION 25

Computer viruses are malicious software programs that infect computers and corrupt or delete the data on them. Identify the virus type that specifically infects Microsoft Word files?

- A. Micro Virus
- B. File Infector
- C. Macro Virus
- D. Boot Sector virus

Answer: C

NEW QUESTION 30

One of the goals of CSIRT is to manage security problems by taking a certain approach towards the customers' security vulnerabilities and by responding effectively to potential information security incidents. Identify the incident response approach that focuses on developing the infrastructure and security processes before the occurrence or detection of an event or any incident:

- A. Interactive approach
- B. Introductory approach
- C. Proactive approach
- D. Qualitative approach

Answer: C

NEW QUESTION 34

Incident management team provides support to all users in the organization that are affected by the threat or attack. The organization's internal auditor is part of the incident response team. Identify one of the responsibilities of the internal auditor as part of the incident response team:

- A. Configure information security controls
- B. Perform necessary action to block the network traffic from suspected intruder
- C. Identify and report security loopholes to the management for necessary actions
- D. Coordinate incident containment activities with the information security officer

Answer: C

NEW QUESTION 39

An assault on system security that is derived from an intelligent threat is called:

- A. Threat Agent
- B. Vulnerability
- C. Attack
- D. Risk

Answer: C

NEW QUESTION 43

Incidents such as DDoS that should be handled immediately may be considered as:

- A. Level One incident
- B. Level Two incident
- C. Level Three incident
- D. Level Four incident

Answer: C

NEW QUESTION 46

Total cost of disruption of an incident is the sum of

- A. Tangible and Intangible costs
- B. Tangible cost only
- C. Intangible cost only
- D. Level Two and Level Three incidents cost

Answer: A

NEW QUESTION 50

Incident prioritization must be based on:

- A. Potential impact

- B. Current damage
- C. Criticality of affected systems
- D. All the above

Answer: D

NEW QUESTION 52

If the loss anticipated is greater than the agreed upon threshold; the organization will:

- A. Accept the risk
- B. Mitigate the risk
- C. Accept the risk but after management approval
- D. Do nothing

Answer: B

NEW QUESTION 57

Absorbing minor risks while preparing to respond to major ones is called:

- A. Risk Mitigation
- B. Risk Transfer
- C. Risk Assumption
- D. Risk Avoidance

Answer: C

NEW QUESTION 59

Adam calculated the total cost of a control to protect 10,000 \$ worth of data as 20,000 \$. What do you advise Adam to do?

- A. Apply the control
- B. Not to apply the control
- C. Use qualitative risk assessment
- D. Use semi-qualitative risk assessment instead

Answer: B

NEW QUESTION 61

What is correct about Quantitative Risk Analysis:

- A. It is Subjective but faster than Qualitative Risk Analysis
- B. Easily automated
- C. Better than Qualitative Risk Analysis
- D. Uses levels and descriptive expressions

Answer: B

NEW QUESTION 63

The correct sequence of Incident Response and Handling is:

- A. Incident Identification, recording, initial response, communication and containment
- B. Incident Identification, initial response, communication, recording and containment
- C. Incident Identification, communication, recording, initial response and containment
- D. Incident Identification, recording, initial response, containment and communication

Answer: A

NEW QUESTION 68

The correct sequence of incident management process is:

- A. Prepare, protect, triage, detect and respond
- B. Prepare, protect, detect, triage and respond
- C. Prepare, detect, protect, triage and respond
- D. Prepare, protect, detect, respond and triage

Answer: B

NEW QUESTION 71

Which of the following is a correct statement about incident management, handling and response:

- A. Incident response is on the functions provided by incident handling
- B. Incident handling is on the functions provided by incident response
- C. Triage is one of the services provided by incident response
- D. Incident response is one of the services provided by triage

Answer: A

NEW QUESTION 72

The service organization that provides 24x7 computer security incident response services to any user, company, government agency, or organization is known as:

- A. Computer Security Incident Response Team CSIRT
- B. Security Operations Center SOC
- C. Digital Forensics Examiner
- D. Vulnerability Assessor

Answer: A

NEW QUESTION 73

The program that helps to train people to be better prepared to respond to emergency situations in their communities is known as:

- A. Community Emergency Response Team (CERT)
- B. Incident Response Team (IRT)
- C. Security Incident Response Team (SIRT)
- D. All the above

Answer: A

NEW QUESTION 76

The free, open source, TCP/IP protocol analyzer, sniffer and packet capturing utility standard across many industries and educational institutions is known as:

- A. Snort
- B. Wireshark
- C. Cain & Able
- D. nmap

Answer: B

NEW QUESTION 77

Changing the web server contents, Accessing the workstation using a false ID and Copying sensitive data without authorization are examples of:

- A. DDoS attacks
- B. Unauthorized access attacks
- C. Malware attacks
- D. Social Engineering attacks

Answer: B

NEW QUESTION 81

To respond to DDoS attacks; one of the following strategies can be used:

- A. Using additional capacity to absorb attack
- B. Identifying non-critical services and stopping them
- C. Shut down some services until the attack has subsided
- D. All the above

Answer: D

NEW QUESTION 83

The message that is received and requires an urgent action and it prompts the recipient to delete certain files or forward it to others is called:

- A. An Adware
- B. Mail bomb
- C. A Virus Hoax
- D. Spear Phishing

Answer: C

NEW QUESTION 86

A Host is infected by worms that propagate through a vulnerable service; the sign(s) of the presence of the worm include:

- A. Decrease in network usage
- B. Established connection attempts targeted at the vulnerable services
- C. System becomes unstable or crashes
- D. All the above

Answer: C

NEW QUESTION 88

The main difference between viruses and worms is:

- A. Worms require a host file to propagate while viruses don't

- B. Viruses require a host file to propagate while Worms don't
- C. Viruses don't require user interaction; they are self-replicating malware
- D. Viruses and worms are common names for the same malware

Answer: B

NEW QUESTION 92

The USB tool (depicted below) that is connected to male USB Keyboard cable and not detected by antispyware tools is most likely called:



- A. Software Key Grabber
- B. Hardware Keylogger
- C. USB adapter
- D. Anti-Keylogger

Answer: B

NEW QUESTION 96

Spyware tool used to record malicious user's computer activities and keyboard strokes is called:

- A. adware
- B. Keylogger
- C. Rootkit
- D. Firewall

Answer: B

NEW QUESTION 98

The individual who recovers, analyzes, and preserves computer and related materials to be presented as evidence in a court of law and identifies the evidence, estimates the potential impact of the malicious activity on the victim, and assesses the intent and identity of the perpetrator is called:

- A. Digital Forensic Examiner
- B. Computer Forensic Investigator
- C. Computer Hacking Forensic Investigator
- D. All the above

Answer: D

NEW QUESTION 100

The person who offers his formal opinion as a testimony about a computer crime incident in the court of law is known as:

- A. Expert Witness
- B. Incident Analyzer
- C. Incident Responder
- D. Evidence Documenter

Answer: A

NEW QUESTION 104

A methodical series of techniques and procedures for gathering evidence, from computing equipment and various storage devices and digital media, that can be presented in a court of law in a coherent and meaningful format is called:

- A. Forensic Analysis
- B. Computer Forensics
- C. Forensic Readiness
- D. Steganalysis

Answer: B

NEW QUESTION 107

Agencies do NOT report an information security incident is because of:

- A. Afraid of negative publicity
- B. Have full knowledge about how to handle the attack internally

- C. Do not want to pay the additional cost of reporting an incident
- D. All the above

Answer: A

NEW QUESTION 109

Business Continuity planning includes other plans such as:

- A. Incident/disaster recovery plan
- B. Business recovery and resumption plans
- C. Contingency plan
- D. All the above

Answer: D

NEW QUESTION 114

The steps followed to recover computer systems after an incident are:

- A. System restoration, validation, operation and monitoring
- B. System restoration, operation, validation, and monitoring
- C. System monitoring, validation, operation and restoration
- D. System validation, restoration, operation and monitoring

Answer: A

NEW QUESTION 118

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

212-89 Practice Exam Features:

- * 212-89 Questions and Answers Updated Frequently
- * 212-89 Practice Questions Verified by Expert Senior Certified Staff
- * 212-89 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * 212-89 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 212-89 Practice Test Here](#)